Lawrence Azegbea

IT Support Specialist · Service Desk · Aspiring Junior SOC Analyst

lawrenceazegbea@gmail.com +353 83 3182 413 Ireland — fully permitted to work

cyberlawr.com github.com/lawr24/cyberlawr linkedin.com/in/lawrence-azegbea-81b802159

CompTIA Security+ certified IT support professional moving into security operations, with hands-on SIEM experience in Microsoft Sentinel and Splunk Enterprise. Built and documented an end-to-end detection pipeline in Sentinel — from Windows event collection through a custom KQL analytics rule to automated incident generation — alongside Active Directory, Linux, Nmap and Wireshark labs. Combines eight years of IT support and troubleshooting with an evidence-based approach to investigation and clear technical documentation.

TECHNICAL SKILLS

SIEM	Microsoft Sentinel · Splunk Enterprise · KQL · SPL · Analytics rules · Log analysis · Incident investigation
CLOUD & IDENTITY	Microsoft Azure · Azure Arc · Azure Monitor Agent · Log Analytics Workspace · Active Directory (AD DS) · Group Policy · DNS
SYSTEMS	Windows Server 2019 · Windows 11 Enterprise · PowerShell · Ubuntu · Kali Linux · Bash · VMware Workstation
NETWORK	Nmap & NSE · Wireshark · TCP/IP · SMB · RDP · Kerberos · LDAP · DHCP · HTTP
IT SUPPORT	Service desk · Endpoint support · User & access management · Technical documentation

CYBERSECURITY PROJECTS

screenshots & methodology at cyberlawr.com

Microsoft Sentinel SIEM — End-to-End Detection Pipeline

Deployed Microsoft Sentinel over an Azure Log Analytics Workspace and onboarded a Windows 11 Enterprise endpoint using Azure Arc and the Azure Monitor Agent. Configured the Windows Security Events connector and Data Collection Rule, verified SecurityEvent ingestion using KQL, then authored a custom analytics rule detecting failed logon attempts that automatically generated a Sentinel incident.

Splunk Enterprise SIEM Lab

Deployed Splunk Enterprise 10.4.2 on Ubuntu and configured continuous monitoring of /var/log, indexing over 33,000 Linux events. Investigated authentication activity using SPL — isolating failed and successful logins and auditing sudo privilege escalation — and profiled hosts, users and source types using stats and top commands.

Windows Server 2019 Active Directory Administration

Deployed a Windows Server 2019 domain controller running AD DS and DNS. Built an enterprise-style Organizational Unit structure with domain users and security groups, linked Group Policy Objects to the IT OU (including restricting Command Prompt access), and joined a Windows 11 Enterprise client to the domain. Diagnosed a failed GPO deployment by systematically validating DNS, connectivity, policy refresh and resource paths rather than rebuilding the environment.

Nmap Enumeration — Windows Server Reconnaissance

Structured reconnaissance from Kali Linux against a Windows Server 2019 target using Nmap 7.95 and the Nmap Scripting Engine — enumerating RPC, NetBIOS, SMB, LDAP, Kerberos, RDP and WinRM with OS and service-version detection, documented to a repeatable methodology.

Wireshark Packet Analysis — Validating SMB Enumeration

Captured live traffic to verify Nmap findings at packet level, analysing TCP handshakes and SMB negotiation to confirm SMB 3.1.1 with signing enabled but not required. Re-scoped to an SMB2 script after an initial script failed during negotiation.

Linux Administration Lab

Administered Kali Linux from the command line: file and permission management, user and group administration, networking commands, process management with ps, and system log review using dmesg and journalctl.

TryHackMe Practical Labs

Ongoing exercises across Windows, Linux, networking and security fundamentals.

PROFESSIONAL EXPERIENCE

Security Professional
Oct 2024 – Present

CCS Security Solutions · Wexford, Ireland

- Monitored and responded to security incidents, ensuring swift and effective resolution.
- Wrote detailed incident reports documenting findings and actions taken.
- Investigated unusual activity to maintain a secure environment for clients.
- Provided customer support while adhering to security procedures under pressure.

AI Trainer
Aug 2021 – Jan 2023

MIIT

- Delivered AI and digital technology training to learner groups, adapting material to varying skill levels.
- Provided technical support, training documentation and data quality assurance for course delivery.

ICT Administrator
Nov 2018 – Sep 2021

Leadership Newspaper

- Installed, configured and maintained Windows desktops and laptops across the organisation.
- Diagnosed and resolved hardware, software and operating system issues, minimising staff downtime.
- Managed user accounts and access permissions in line with IT policy.

Cybersecurity Awareness Educator
Apr 2016 – Sep 2018

Cyber Security Challenge Nigeria (CYSEC NG)

- Delivered awareness sessions on phishing, password security and safe online practices.

IT Support Technician
Jun 2011 – Nov 2014

DAN Blaise Communications

- Installed and maintained Windows systems; diagnosed and resolved hardware, software and OS faults.

CERTIFICATIONS

CompTIA Security+ · Network+ · A+ · Tech+ · Secure Infrastructure Specialist (CSIS) · IT Operations Specialist (CIOS)
Microsoft Career Essentials in Cybersecurity · First Aid Responder · Community First Responder (Advanced)

EDUCATION

BSc Computer Science
Mar 2018 – Jan 2023

Ekiti State University, Ado Ekiti, Nigeria

BSc Biochemistry — Second Class Upper Division
Jan 2014 – Feb 2018

Ambrose Alli University, Nigeria

VOLUNTEER EXPERIENCE

Order of Malta (Community First Responder) · Balseskin Community Service · Sanctuary Runners · Five Lamps Arts Festival (Invigilator)